ATTACHMENT A

Place to be Searched

The residence at **410 Turquoise Court, Mascoutah, St. Clair County, Illinois**, as pictured below and described as a two-story single family residence with attached garage, displaying the number 410 on the exterior wall between the garage and front door.

ATTACHMENT B

Property to be seized

1. All records constituting evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030, specifically:

a) All records, information, and communications relating to the accounts, domains, computers, or servers under the custody and control of the agency;

b) All records, information, and communications relating to the unauthorized accessing of any accounts, domains, computers, or servers;

c) All records, information, and communications relating to collecting or acquiring information about government accounts, domains, computers, or servers;

d) All records, information, and communications showing contact with service providers hosting government accounts, domains, computers, or servers;

e) All records, information, and communications software or computer code used to compromise any accounts, domains, computers, or servers;

f) All records and information identifying the person(s) having custody or control over the premises searched, evidence seized (including digital devices), Victim domains or accounts; or accounts used by Jamie Magers, Brian Wohlwinder, and any others involved in violations of 18 U.S.C. § 1030;

g) Computers or storage media used as a means to commit the violations described above, including violations of 18 U.S.C. § 1030

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a) evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b) evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c) evidence of the lack of such malicious software;

d) evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f) evidence of the times the COMPUTER was used;

g) passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h) documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i) records of or information about Internet Protocol addresses used by the COMPUTER;

j) records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k) contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

FILED

SEP 23 2013

CLIFFORD J. PROUD
U.S. MAGISTRATE JUDGE
SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS OFFICE

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IN RE SEARCH OF	)	
410 TURQUOISE COURT,	)	**Case No.** 13-M-6048-CSP
MASCOUTAH, ILLINOIS	)	
	)	**FILED UNDER SEAL**
	)	

AFFIDAVIT IN SUPPORT OF APPLICATION
FOR SEARCH WARRANT

Your Affiant, Christopher D. Trifiletti, being duly sworn, deposes and states the following:

INTRODUCTION

1. This affidavit is submitted in support of an application for a search warrant, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, to search the residence at **410 Turquoise Court, Mascoutah, Illinois**, a two-story single family residence with attached garage, displaying the number 410 on the exterior wall between the garage and front door (a photo of which appears in Attachment A), for evidence of federal offenses, including:

Title 18, U.S.C. § 1030 – Fraud and related activity in connection with computers

Whoever . . .

(a)(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (B) information from any department or agency of the United States; or (C) information from any protected computer;

(a)(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States; . . .

(a)(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result

of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if — (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States;

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section [shall be guilty of a crime.]

2. Your Affiant is a Special Agent with the Federal Bureau of Investigation (FBI), and has been so employed for the past fourteen and a half years. I am currently assigned to the Cyber Squad of the Springfield Field Office and have completed numerous computer intrusion investigations. I have executed search warrants on computers, email accounts, residences, and various types of other digital facilities, conducted review of various types of computer and network logs, interviewed witnesses and subjects related to intrusion investigations, and secured other relevant information using other investigative techniques. I have completed numerous basic and advanced cyber investigative trainings gaining an understanding of the fundamentals of computer hardware, operating systems, computer networks, hacking and malware, information security, and the processing of electronic evidence.

3. The facts set forth in this affidavit are based on your Affiant's personal knowledge, knowledge obtained from other investigators and witnesses, and records and reports. Your Affiant has not included every fact known through the course of the investigation within this affidavit but has included those facts your Affiant believes are sufficient to establish probable cause that the violations set forth above have occurred, and the emails accounts contain evidence, fruits, and/or instrumentalities of violations.

4. As set forth below, there is probable cause to believe that a search of the residence listed above will uncover evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1030.

STATEMENT OF FACTS

5. On or about September 3, 2013, United States government personnel working in Maryland discovered that they had lost access to an email account, and a domain[1] originally under the control of a department of the United States government (the "Victim"). Upon attempting to regain access to the email account, Victim personnel realized that the password to the account had been changed and the security challenge question used for password recovery had also been changed. Victim personnel also determined that the password for the account controlling the domain was changed as well.

6. While conducting additional research into the loss of access to these accounts, investigators also observed unusual Internet traffic involving several other domains controlled by the Victim. The domains described in this Affidavit were used by a division of the Victim that engages in "penetration testing." This division's mission, in part, is to test the networks of other government networks to look for security vulnerabilities, including networks operated by agencies within the Department of Defense. To accomplish this, the division – among other things – is authorized to attempt to access government networks covertly.

7. Investigators determined that this anomalous traffic was malicious. Investigators found that a feature of the software running on the Victim's domains was being exploited so as to

[1] The domains discussed in this affidavit are website domains, of the type that appears in the location box at the top of an Internet browser with the prefix "HTTP" (e.g., http://www.fbi.gov). The domains discussed in this affidavit were each maintained on the server of a commercial web-hosting company. Commercial web-hosting companies maintain server computers connected to the Internet for the purpose of hosting website domains. Customers can create an account with the company, and then pay the company to use the web-hosting company's servers to operate websites on the Internet. Victim personnel registered these domains, rented server space from the web-hosting companies, and then controlled those domains through an account with the web-hosting company (except where, as noted here, unauthorized control of a domain was obtained by a third party).

harvest information, including account password, from Victim personnel each time they logged into a domain that was targeted by this exploit. For at least a few of the domains targeted by this exploit, the illicitly obtained information was being transmitted to the compromised email account.

8. As is the common practice with network security professionals, investigators searched a database that contains records of historical network activity for the Victim's networks, and those of its associated organizations, for other information relating to this activity. Those searches were authorized by the pre-existing consent of those networks' users, who all acknowledge on a regular basis that their communications are subject to monitoring for precisely that purpose. This notice and consent were provided, *inter alia*, by banners that alerted the networks' users that the network was monitored.

9. That search revealed a document that contained information about the compromised email account and the compromised domain. The document also identified a number of other domains and email accounts controlled by the Victim. This information is not publicly available. In the document, some of the Victim's domains were marked with an "X." Additional investigation revealed that the domains marked with an "X" in the document were many of the same domains affected by this malicious activity. In addition to domains controlled by the Victim, the document identified domains under the custody and control of other government agencies. Investigators analyzed the document's metadata, and it showed that the author was "Jamie Magers."

10. Investigators were also able to identify some IP addresses involved in the malicious Internet traffic. Two of these IP addresses are registered to computers at Scott Air Force Base, Illinois. A check of Air Force records showed that a "Jamie Magers" is now employed as a

contractor at Scott Air Force Base. Magers is employed as a cyber-security specialist, assigned to a "hunt team" for Defense Information Systems Agency ("DISA"). The so-called hunt team is tasked with detecting unauthorized intrusions into Department of Defense networks (i.e. "hacking"). Magers is therefore very familiar with cyber-security matters. The Victim has confirmed that Jamie Magers is not authorized to access the domains or email account affected by this malicious activity.

11. A records check of law enforcement databases showed that Magers resides at **410 Turquoise Court, Mascoutah, Illinois**.

12. Investigators also identified an IP address involved in the malicious traffic that was registered to an Internet Service Provider ("ISP"). In response to a subpoena, on Friday, September 13, 2013, the ISP produced the name and address of the subscriber for that IP address from June 1, 2013 to September 10, 2013 (the date range requested by the subpoena). That information showed that during that period, the IP address was assigned to Magers's residence at **410 Turquoise Court, Mascoutah, Illinois**, and that the account was registered in the name of a woman also living at that residence.

13. Additional investigation showed that the document discussed above was sent from the email account d3adg0d@gmail.com, which was accessed from the network of an affiliated government agency. Further investigation into the use of this email account on the network of the Victim and its affiliated government networks indicated that the account was controlled by Jamie Magers. For instance, d3adg0d@gmail.com was also used, from the network of an affiliated government agency, for online shopping to make a purchase for Jamie Magers.

14. A search of the Victim's databases also revealed a log of an online chat that was transmitted on the network of an affiliated government agency, between Jaime Magers, using the

account d3adg0d@gmail.com, and Brian Wohlwinder, using the account Brian@Wohlwinder.com. In that chat, Magers and Wohlwinder had the following exchange:

Magers: Dude, I have something epic!
Magers: BRIAN!!!
Magers: your missing out on some good stuff
Magers: Yeah. Passwords, logons, access to servers
. . .
Magers: Had some new [Victim] domains
Wohlwinder: Me to. I'm doing ia forward hit me up when you get to work tomorrow, we can exchange intel

Magers and Wohlwinder went on to arrange further communications on a different network. Records suggest the chat partially transcribed above took place in or about late August 2013.

15. A search of the Victim's databases also revealed a screenshot ofd3adg0d@gmail.com having been accessed on the network of an affiliated government agency. That screenshot contained a "last-accessed" notation referencing the IP address assigned to Magers' residence through at least September 10, 2013, at **410 Turquoise Court, Mascoutah, Illinois**. Based on my training and experience, it is reasonable to infer that any malicious network activity conducted by Magers through his d3adg0d@gmail.com account may have occurred both on his government systems as well as any of his home computing devices.

16. A records check showed that Wohlwinder is also an Air Force contractor, but is stationed at Shaw Air Force Base. Further checks showed that Magers once worked at Shaw Air Force Base at the same time Wohlwinder was employed there. The Victim has confirmed that Brian Wohlwinder is not authorized to access the domain or email accounts affected by this malicious activity.

17. Logs from the Victim's database showed additional communication between Magers and Wohlwinder, when Wohlwinder sent an email from both his personal email account,

Brian@Wohlwinder.com, and a government email account assigned to Wohlwinder, to Magers at d3adg0d@gmail.com. The subject line of the email was "files to Jamie".

18. As noted above, the document described in paragraph 9 listed not only domains controlled by the Victim, but also domains controlled by affiliated government agencies, including the Navy and Air Force. Personnel at the Victim therefore decided to alert the affiliated government agencies of the possible breach and unauthorized access to these domains. Starting on September 9 or 10, Victim personnel began notifying affiliated agencies of the breach. Among the agencies notified were the Naval Criminal Investigative Service and the Air Force Office of Special Investigations. Initially those notifications were made to only a few individuals, but over the course of that week more personnel were notified. Magers is employed as a contractor for the Air Force, assigned to the Defense Information System Agency (DISA).

19. On September 12, 2013, Victim personnel were notified by Jamie Magers' supervisor that Magers wanted to report vulnerabilities in the Victim's electronic infrastructure, including domains. The next day, on September 13, Victim personnel held a conference call with Magers and his supervisor, and other members of the Scott Air Force Base DISA hunt team. An FBI agent was present for that call, although Magers and his co-workers were not aware of the agent's presence. In that call, Magers' supervisor again noted that Magers had reported to the supervisor the previous day, September 12, that Magers had found security flaws in the Victim's accounts and domains, and the supervisor therefore contacted the Victim. The supervisor indicated that Magers wanted to explain the scope of the security flaws to Victim personnel.

20. Victim personnel advised Magers that they needed to know the scope of any security flaws, and precisely what actions Magers had taken. Victim personnel emphasized that accurate information about Magers actions was especially important, so as the personnel took remedial

steps and identified unauthorized intrusions, they would be able to determine whether any security breaches were attributable to Magers or to external adversaries, such as foreign governments.

21. Magers then explained that he had identified security flaws in the Victim's accounts and, that in order to assist the Victim, had taken a number of steps. He stated that he spent weeks collecting information, and now wanted to assist the Victim by explaining what he did and what he found. Magers explained that he took control of the Victim's compromised email account, after finding that it was expired, and simply re-registered it under his control. He then took control of the Victim's domain linked to that email account by requesting a password reset from the web-hosting company, which was sent to the compromised email account, the account Magers now controlled. He then reset the password to the account controlling the domain, and assumed control over the domain as well. (The investigation indicated this information is true).

22. He also explained the means by which he identified the Victim's accounts. As part of his investigative method, Magers indicated that he did Internet searches using Google's search engine. Magers provided copies of searches of public information obtained via Google searches that assisted him in identifying Victim's domains. Magers also provided a partial copy of the information in the document described in paragraph 9.

23. On several key points, Magers' explanation was inconsistent with the information uncovered during the course of the investigation thus far.

a) Magers claimed that he took control of the compromised domain because it was expired, and he therefore wanted to "secure" the domain for the Victim. But Victim personnel have confirmed that the domain is not scheduled to expire until January 2014.

b) Magers was also asked what he did with the compromised email account, after he took control. He claimed that he did not use the account, except for something related to the use of Twitter. But, as noted above in paragraph 7, investigators have determined the software on several Victim domains was exploited to harvest login information, including passwords, from Victim personnel and, in at least some cases, that information was transmitted to the compromised email account.

c) Although Magers advised he identified a number of other Victim domains and accounts, he claimed he never attempted to access those other domains and accounts, or obtain any information from them. When asked, Magers admitted that he had found a security vulnerability in the software for the domain he took over, and that he had tested that vulnerability once against that domain. But he claimed that he never used that security flaw against any of the Victim's other domains. He reiterated that he did not access any domains or accounts except the first compromised email and domain account, obtain any information from other Victim domains, or attempt to alter or exploit the software for those domains. However, as described above, investigators have determined that IP addresses assigned to Scott Air Force Base and assigned to Magers' residence were used for malicious activity to harvest login credentials from several Victim domains.

d) After Magers provided the password for the compromised email account, an FBI agent logged into the account. The account initially showed only a single email received. However, in the lower part of the screen was a message asking the user if s/he wished to restore several recently deleted emails. (I know through training and experience that the option to restore recently deleted emails is a common feature of email software). An FBI agent restored

the recently deleted emails, and more than a dozen emails were restored. These emails contained login credentials, including passwords, which Victim personnel used to access multiple domains.

e) Magers also claimed that he informed no one of the so-called security flaws in the Victim's accounts and domains until he told his supervisor, the previous day, September 12. When asked, he confirmed that he shared this information with no one until September 12 and then only with his supervisor, that no one else was involved in collecting this information, and that no one else knew of his activities until September 12. As noted above in paragraph 14, however, in a log of a chat log between Magers and Wohlwinder, Magers specifically stated that he had "Passwords, logons[sic], access to servers[,]" and Wohlwinder stated that he also had Victim domains. That communication occurred in or about late August 2013.

24. During the September 13 conference call noted in paragraph 19 , Victim personnel also asked Magers what IP addresses he had used for activities relating to Victim domains. Magers stated that all of his activity came from IP addresses at Scott Air Force base or an "un-attributable" IP address (un-attributable in the sense that it is an IP controlled by the government but not publicly listed as government-controlled). Agency personnel asked for a list of all IP addresses Magers used. Magers later provided several IP addresses, including the IP address assigned to the residence through at least September 10, 2013 at **410 Turquoise Court, Mascoutah, Illinois.**

25. As noted above, the Victim began to notify affiliated agencies of the security breach on September 9 and 10, 2013 – including Department of Defense agencies such as the Air Force, the agency that employs Magers and Wohlwinder. Based on my training and experience I know that the cyber-security components at Scott Air Force Base, including DISA, are a tightly-knit community, as with many other government agencies. I also know, that shortly after these

notifications began, Magers approached his supervisor about his activities identifying – and, in at least one case, taking control of – Victim email and domain accounts. This occurred even though Magers stated that he had been collecting this information for weeks. I believe it is reasonable to infer that after information about the security breach was disseminated to Department of Defense agencies, Magers (and/or conspirator(s)) became aware that the Victim was investigating this security breach, which would explain the timing of his (partial) disclosure to his supervisor and the Victim.

26. On September 20, 2013, a vehicle registered to Jamie Magers was observed parked in the attached garage at **410 Turquoise Ct., Mascoutah, IL**. This was observed from the public street as the garage door was open.

27. I know through my training, knowledge and experience, that individuals commonly store their possessions, including digital devices such as computers, at their residences. In addition, I know through my training and experience that computer and cyber professionals are very likely to have digital devices, such as computers, in their residence. As set forth above, I believe there is probable cause to believe that Magers possesses digital devices, such as computers, at his home that are capable of accessing the Internet. Furthermore, there is probable cause to believe that Magers has used those digital devices in the course of his activities relating to unauthorized access of the Victim domains and accounts.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four

numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

29. As described above and in Attachment B, this application seeks permission to search for records that might be found at the residence at **410 Turquoise Court, Mascoutah, Illinois** ("PREMISES"), in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

30. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how

computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f) I know that when an individual uses a computer to obtain unauthorized access to a victim computer, domain, or account over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used;

data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on

the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

34. Based upon the information contained in this affidavit, your Affiant submits that probable cause exists to believe that the residence at **410 Turquoise Court, Mascoutah, Illinois**, contains the evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1030.

FURTHER AFFIANT SAYETH NAUGHT.

Christopher D. Trifiletti, Special Agent
FBI

Subscribed and sworn to before me this 23rd day of September, 2013.

Hon. Clifford J. Proud
United States Magistrate Judge

STEPHEN R. WIGGINTON
United States Attorney

BRUCE E. REPPERT
Assistant United States Attorney